# Communication Session Encryption And Authentication System

## ABSTRACT

An interactive mutual authentication protocol, which does not allow shared secrets to pass through untrusted communication media, integrates an encryption key management system into the authentication protocol, so that key management becomes an essential part of the authentication protocol itself. The system provides a secure distribution of a secret session random key used in symmetric cryptography. Successful exchange of this encryption key allows for secure transit of the protocol data over communication lines in encrypted form, permitting explicit mutual authentication of the connected parties. The post-authentication stage of the communication session can use secure encryption for the data exchange, since each party has already obtained the secret session random key.